Google™ Advanced Search Preferences Language Tools Search Tips

luc derive xtr Google Search

Web · Images · Groups · Directory · News ·

Searched the web for **luc derive xtr**. Results **1** - **10** of about **18**. Search took **0.23** seconds.

Tip: In most browsers you can just hit the return key instead of clicking on the search button.

Citations: The **XTR** public key system - Lenstra, Verheul (...

... ...has been used in [30] to **derive** some results ... AK Lenstra and ER Verheul, The **XTR** public key system ... compression methods based on traces such as **LUC** [109] and ...

citeseer.nj.nec.com/context/1224892/308852 - 24k - Supplemental Result - Cached - Similar pages

[PDF] Hidden Number Problem in Small Subgroups

File Format: PDF/Adobe Acrobat - View as HTML

... As in [1, 5] we apply our algorithm for the hidden number problem to **derive** a bit security result for the Diffie-Hellman scheme. ...

venona.antioffline.com/2003/049.pdf - Similar pages

[PDF] Unbelievable Security Matching AES security using public key ...

File Format: PDF/Adobe Acrobat - View as HTML

... character- istic and compressed representation methods (**LUC** [?] and **XTR** ... included, with the exception of **XTR** – it is ... To **derive** such a bound the approach from ...

www.win.tue.nl/~klenstra/aes_match.pdf - Similar pages

[PS] Unbelievable Security Matching AES security using public key

File Format: Adobe PostScript - View as Text

... character- istic and compressed representation methods (**LUC** [17] and ... not included, with the exception of **XTR** - it is ... To **derive** such a bound the approach from [7 ...

www.win.tue.nl/~klenstra/aes_match.ps - Similar pages

[More results from www.win.tue.nl]

[PDF] Introduction

File Format: PDF/Adobe Acrobat - View as HTML

... 342, 518, 521] to the secret key of the **XTR** [332, 333, 334, 335, 551] and to the **LUC** [47, 536] key exchange protocols. We apply our method to **derive** quite a ...

www.birkhauser.ch/books/math/6654-0_Introduction.pdf - Similar pages

[PS] Future directions in algorithmic number theory

File Format: Adobe PostScript - View as Text

... The Hi **derive** from injective resolutions on the etale topology. ... and compare TBC with Lucas-based cryptosystems and **XTR**, and understand **LUC**, **XTR**, and Beyond ...

www.aimath.org/WWN/primesinp/primesinp.ps - Similar pages

[PDF] Future directions in algorithmic number theory

File Format: PDF/Adobe Acrobat - View as HTML

Page 1. Future directions in algorithmic number theory The American Institute of Mathematics This is a hard–copy version of a web ...

www.aimath.org/WWN/primesinp/primesinp.pdf - Similar pages

Cryptography-Digest Digest #942

... eg DH over GF(p), ECC, **LUC***, or **XTR**) would be ... (Note: I'm not particularly recommending **LUC**. ... changing 256-element permutation that is used to **derive** output. ...

www.mail-archive.com/cryptography-digest@senator-bedfellow.mit.edu/ msg03144.html - 36k - Supplemental Result - Cached - Similar pages

Citations: A Public Key Cryptosystem and a Signature Scheme based ...
... Then we will investigate their touching point and **derive** practical consequences. ... 19 5.3 **XTR** . ... includes RSA [39] Rabin [38] Williams [42, 43] **LUC** [41] Kurosawa ...
citeseer.ist.psu.edu/context/5705/0 - 62k - Cached - Similar pages

Molecular Endocrinology -- Furlow and Brown 13 (12): 2076
... It has been difficult to **derive** generalizations about the ... For cotransfection of TR expression vectors, **xTR** A and ... g reporter construct (TREs in MTV-**Luc**) or 0.1 ...
mend.endojournals.org/cgi/content/full/13/12/2076 - Similar pages

Google ▶
Result Page: 1 2 **Next**

Google Advanced Search Preferences Language Tools Search Tips

lucdif Google Search

Web · Images · Groups · Directory · News ·

Searched the web for **lucdif**. Results **1** - **10** of about **315**. Search took **0.22** seconds.

Tip: In most browsers you can just hit the return key instead of clicking on the search button.

Speed Comparison of Popular Crypto Algorithms
... **LUCDIF** 512 Key-Pair Generation, 1913, 2.003, 1.05. **LUCDIF** 512 Key-Pair Generation with precomputation, 1897, 2.003, 1.06. **LUCDIF** 512 Key Agreement, 1078, 2.003, 1.86. ...
www.eskimo.com/~weidai/benchmarks.html - 15k - Cached - Similar pages

// luc.cpp - written and placed in the public domain by Wei Dai # ...
... k(rng, 1, q-1, Integer::ANY); r = Lucas(k, g, p); s = (k + x*(r+m)) % q; } // * **LUCDIF**::**LUCDIF**(const ...
cvs.sourceforge.net/viewcvs.py/cryptopp/ src/luc.cpp?rev=1.1.1.3 - 11k - Cached - Similar pages

#ifndef CRYPTOPP_LUC_H #define CRYPTOPP_LUC_H /** \file */ # ...
... class **LUCDIF** : public PK_SimpleKeyAgreementDomain { public: **LUCDIF**(const Integer &p, const Integer &g); **LUCDIF**(RandomNumberGenerator &rng, unsigned int pbits ...
cvs.sourceforge.net/viewcvs.py/ cryptopp/src/luc.h?rev=1.3 - 9k - Cached - Similar pages
[More results from cvs.sourceforge.net]

Citations: Cryptanalysis of the Dickson scheme - Muller, Nobauer ...
... coincides with the variant of the Di#eHellman key exchange scheme that was proposed and analyzed by a series of authors; 15] where the name **LUCDIF** was proposed ...
citeseer.nj.nec.com/context/177540/0 - 11k - Cached - Similar pages

Cryptography-Digest Digest #936
... com> Subject: Re: XTR independent benchmarks Date: Sun, 4 Jun 2000 13:43:43 +0200 > > First of all, the hard part of parameter generation in **LUCDIF** consists of ...
www.mail-archive.com/cryptography-digest@senator-bedfellow.mit.edu/ msg03138.html - 29k - Cached - Similar pages

Cryptography-Digest Digest #929
... 4.19 DH 1024 Agreement 10.53 DH 2048 Key-Pair Generation 46.91 DH 2048 Key-Pair Generation with precomputation 14.10 DH 2048 Agreement 47.82 **LUCDIF** 512 Key ...
www.mail-archive.com/cryptography-digest@senator-bedfellow.mit.edu/ msg03131.html - 29k - Cached - Similar pages
[More results from www.mail-archive.com]

SourceForge.net: File Release Notes and Changelog
... Twofish, Serpent SEAL, Luby-Rackoff, MDC, various encryption modes (CFB, CBC, OFB, counter), DH, DH2, MQV, DSA, NR, ElGamal, LUC, **LUCDIF**, LUCELG, Rabin, RW, RSA ...
https://sourceforge.net/project/ shownotes.php?release_id=22178 - 33k - Cached - Similar pages

Algorithm
... **LUCDIF** 512 Key-Pair Generation, 281, 1.000, 3.56. **LUCDIF** 512 Key-Pair Generation with precomputation, 287, 1.000, 3.48. **LUCDIF** 512 Key Agreement, 200, 1.000, 5.00. ...
www.stud.ntnu.no/~tlan/ test2.stud.ntnu.no-benchmark.html - 12k - Cached - Similar pages

[PDF] Efficiency Analysis and Comparison of Public Key Algorithms

File Format: PDF/Adobe Acrobat - View as HTML
... ECIEC) Elliptic Curve Digital Signature Algorithm (ECDSA) Elliptic Curve Nyberg-Rueppel (ECNR) Public Key Cryptography Algorithms Other: **LUCDIF** LUCELG LUCRSA ...
www.mit.bme.hu/~csilla/CSCS2002/EC_prezentacio.pdf - Similar pages

[PS] Doing More with Fewer Bits
File Format: Adobe PostScript - View as Text
... 2 A different view of the **LUCDIF** cryptosystem Central in the construction of the **LUCDIF** variant of the Diffie-Hellman keyexchange scheme is a * 512-bit prime ...
www.win.tue.nl/~ruudp/paper/36.ps - Similar pages

Gooooooooogle ▶
Result Page: 1 2 3 4 5 6 7 8 9 10 **Next**

lucdif Google Search Search within results

Dissatisfied with your search results? Help us improve.

Get the Google Toolbar: 

Google Advanced Search Preferences Language Tools Search Tips

"luc a new public key system" Google Search

Web · Images · Groups · Directory · News ·

Searched the web for **"luc a new public key system"**. Results **1** - **10** of about **87**. Search took **0.25** seconds.

LUC: A New Public Key System - Smith, Lennon (ResearchIndex)
... nj.nec.com/228891.html More @techreport{ smith93luc, author = "Peter Smith and Michael JJ Lennon", title = "{**LUC**}: {**A**} **New Public Key System**", year = "1993 ...
citeseer.nj.nec.com/228891.html - 22k - Cached - Similar pages

A New and Optimal Chosen-message Attack on RSA-type Cryptosystems ...
... Koyama, Maurer et al. - 1991 25 A new elliptic curve based analogue of RSA (context)
- Demytko - 1994 17 **LUC**: **A new public key system** - Smith, Lennon 16 ...
citeseer.nj.nec.com/bleichenbacher97new.html - 24k - Cached - Similar pages
[More results from citeseer.nj.nec.com]

[PDF] **LUC: A New Public Key System** 1. Public Key Encryption
File Format: PDF/Adobe Acrobat - View as HTML
LUC: **A New Public Key System** Peter J. Smith a and Michael JJ Lennon b a LUC Partners, Auckland UniServices Ltd, The University of Auckland, Private Bag 92019 ...
preterhuman.net/texts/cryptology/LUC_PUBL.PDF - Similar pages

LUC
... January 1993. PJ Smith, MJJ Lennon, "**LUC** : **A New Public Key System**", Proceedings of the Ninth IFIP International Symposium on Computer Security '93, pp. ...
www.kisa.or.kr/technology/sub1/LUC.htm - 14k - Cached - Similar pages

XTR
... http://home.hetnet.nl/~ecstr/mathdetails.htm. PJ Smith, MJJ Lennon, "**LUC** : **A New Public Key System**," Proceedings of the Ninth IFIP International Symposium on ...
www.kisa.or.kr/technology/sub1/XTR.htm - 14k - Cached - Similar pages

[PS] GROUPE REGARDS
File Format: Adobe PostScript - View as Text
... the ACM, (Feb. 1978), 21, (2), 120-126. [3] smith, pj, and lennon, mjj: `**LUC**: **A new public key system**',. in Ninth IFIP Symposium ...
cnscenter.future.co.kr/resource/crypto/ algorithm/pkc/CG1997_8.ps - Similar pages

Lucas sequences and cryptography
... FTP archive at funet (Incl. papers and source code); Papers: LUC [[citeseer]]: **LUC**: **A New Public Key System** (Peter J. Smith, Michael JJ Lennon, 1993). ...
www.tcs.hut.fi/~helger/crypto/link/public/luc.html - 6k - Cached - Similar pages

Published in R. Whright and P. Neumann, eds, Network Threats, ...
... 1976 2 **LUC**: **A new public key system** (context) - Smith, Lennon - 1993
2 Graduate Texts in Mathematics (context) - in, theory et al. ...
gunther.smeal.psu.edu/20562.html - 27k - Cached - Similar pages

[PS] To appear in Journal of Cryptology.
File Format: Adobe PostScript - View as Text
... [19] PJ Smith and MJJ Lennon. **LUC**: **a new public key system**. In EG Douglas,editor, Proceedings of the Ninth IFIP Symposium on Computer Security, pp. 103-. 117. ...
www.ee.tku.edu.tw/~lcis/people/joye/ publications/chinese.ps.gz - Similar pages

[PS] **LUC**: **A New Public Key System** Peter J. Smitha and Michael JJ ...
File Format: Adobe PostScript - View as Text
LUC: **A New Public Key System** Peter J. Smitha and Michael JJ Lennonb aLUC Partners, Auckland UniServices Ltd, The University of Auckland,Private Bag 92019 ...
sunsite.bilkent.edu.tr/pub/security/cryptography/ doc/luc-public-key-paper.ps.gz - Similar pages

Goooogle ▶
Result Page: 1 2 3 4 **Next**

"luc a new public key system" Google Search Search within results

Dissatisfied with your search results? Help us improve.

Get the Google Toolbar: 

Google Home - Advertise with Us - Business Solutions - Services & Tools - Jobs, Press, & Help

L Number	Hits	Search Text	DB	Time stamp
2	24	seroussi.in.	USPAT	2003/11/26 13:00
3	1294	380/30.ccls. 713/168,180.ccls. 708/490.ccls.	USPAT	2003/11/26 13:01